REMARKS

Claim 1 was pending in the application. Claim 1 is amended. Claims 2-40 are added. Claims 1-40 are now pending in the application. Claims 1, 7, 21, and 27 are the independent claims. The specification is amended to cross-reference related applications. Entry of the Amendment and substantive examination of the application are respectfully requested.

Claims in excess of those paid for with the filing fee are added by this amendment. A check is enclosed in payment of the fee for the excess claims. If the check is missing, or made out for an insufficient amount, please charge any deficiency to our deposit account, No. 501998, and notify us accordingly.

Respectfully submitted,

George Wallace

April 30, 2002

George F. Wallace
Attorney for Applicant
Reg. No. 45,286

Date

IP STRATEGIES, P.C.
806 7th Street, N.W.
Suite 301
Washington, D.C. 20001
202/289-2700 (Voice)
202/289-3594 (Facsimile)

Marked-up Copy of Specification and Claims

In the Specification:

Beginning on page 1 at line 2:

Cross-Reference to Related Patents and Applications

This is related to U.S. Provisional Patent Application Serial No. 60/098,915, filed on September 1, 1998, priority of which is claimed under 35 U.S.C. §119. This is also related to U.S. Patent No. 5,375,169, entitled "Cryptographic Key Management Method and Apparatus," which issued on December 20, 1994 to SCHEIDT et al., to U.S. Patent No. 5,787,173, entitled "Cryptographic Key Management Method and Apparatus," which issued on July 28, 1998 to SCHEIDT et al., and to U.S. Patent No. 6,229,445, entitled "RF Identification Process and Apparatus," which issued on May 8, 2001 to WACK. This is also related to the following co-pending U.S. patent applications: Serial No. 08/974,843, entitled "Cryptographic Medium," filed on November 20, 1997 by WACK et al.; Serial No. 09/023,672, entitled "Cryptographic Key Split Combiner," filed on February 13, 1998 by SCHEIDT et al.; Serial No. 09/874,364, entitled "Cryptographic Key Split Combiner," filed on June 6, 2001 by SCHEIDT et al.; Serial No. 09/917,795, entitled "Cryptographic Key Split Combiner," filed on July 31, 2001 by SCHEIDT et al.; Serial No. 09/917,794, entitled "Cryptographic Key Split Combiner," filed on July 31, 2001 by SCHEIDT et al.; Serial No. 09/917,802, entitled "Cryptographic Key Split Combiner," filed on July 31, 2001 by SCHEIDT et al.; Serial No. 09/917,807, entitled

"Cryptographic Key Split Combiner," filed on July 31, 2001 by SCHEIDT et al.; Serial No. 09/992,529, entitled "Cryptographic Key Split Binder for Use With Tagged Data Elements," filed on November 20, 2001 by SCHEIDT et al.; Serial No. 09/421,293, entitled "Secure Accounting and Operational Control and Reporting System," filed on October 20, 1999 by KOLOUCH; Serial No. 09/205,221, entitled "Access Control and Authorization System," filed on December 4, 1998 by Scheidt et al.; Serial No. 09/418,806, entitled "Cryptographic Information and Flow Control," filed on October 15, 1999 by WACK et al.; Serial No. 09/936,315, entitled "Voice and Data Encryption Method Using a Cryptographic Key Split Combiner," filed on September 10, 2001 by SCHEIDT; Serial No. 10/035,817, entitled "Electronically Signing a Document," filed on October 25, 2002 by SCHEIDT et al.; Serial No. 10/060,039, entitled "Multiple Factor-Based User Identification and Authentication," filed on January 30, 2002 by SCHEIDT et al.; and Serial No. 10/060,011, entitled "Multiple Level Access System," filed on January 30, 2002 by SCHEIDT et al.

The paragraph beginning at page 1, line 7:

[Priority is claimed under 35 U.S.C. §119 of U.S. provisional patent application 60/098,915, filed on September 1, 1998, now abandoned.]

The paragraph bridging pages 21 and 22:

The SuperCard™ is an ISO complaint smart card that has enhanced processing ability and greater memory than current smart cards. It includes tamper resistance and hardware random number generation. The processing capability internal to the card may be used to reduce CKM task processing on the workstation. Even though the bandwidth between the card and the workstation is limited, with CKM only small amounts of data [re]are transferred between the two. Larger memory within the card also makes it possible to store user credential files, as well as "private" CKM applications.

In the Claims:

1. (Amended) A method of encrypting an object, comprising:

combining a plurality of key splits to generate [generating] a cryptographic key;

[using the cryptographic key to initialize] initializing a cryptographic algorithm with the cryptographic key; and

applying the initialized cryptographic algorithm to the object, to form an encrypted object;

wherein [the key is generated by combining key splits, wherein] at least one of the plurality of key splits [is a biometric value corresponding to a particular person] corresponds at least in part to a biometric measurement.

2. The method of claim 1, further comprising:

for at least one of the plurality of key splits, adding the at least one key split to the encrypted object.

3. The method of claim 1, further comprising:

for at least one of the plurality of key splits, adding reference data associated with the at least one key split to the encrypted object.

4. The method of claim 1, further comprising retrieving at least one of the plurality of key splits from a storage medium.

5. The method of claim 4, wherein the storage medium is disposed on a smart card.

6. The method of claim 1, wherein combining a plurality of key splits to generate a cryptographic key is performed on a smart card.

7. In a cryptographic system associated with an organization, a method of encrypting an object by a user, comprising:

generating a first cryptographic key by combining an organization split corresponding to the organization, a maintenance split, a random split, and at least one label split;

initializing a cryptographic algorithm with the first cryptographic key;

encrypting the object according to the initialized cryptographic algorithm;

adding combiner data to the encrypted object, wherein the combiner data includes

reference data corresponding to at least one of the at least one label split and the cryptographic algorithm,

name data associated with the organization,

at least one of the maintenance split and a maintenance level associated with the maintenance split, and

the random split; and

storing the encrypted object with the added combiner data.

8. The method of claim 7, further comprising selecting the at least one label split from at least one credential.

9. The method of claim 8, wherein the selected at least one label split is encrypted, and the method further comprises:

deriving a second cryptographic key from a user ID associated with the user, a password associated with the user, and at least one of a unique data instance and a random value, and

decrypting the selected at least one label split with the second cryptographic key.

10. The method of claim 8, wherein the at least one credential is retrieved from a memory.

11. The method of claim 10, wherein the memory is disposed on a smart card.

12. The method of claim 8, further comprising generating a time stamp corresponding to a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

13. The method of claim 8, wherein the combiner data further includes a user ID associated with the user.

14. The method of claim 7, further comprising generating a time stamp representing a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

15. The method of claim 7, wherein the combiner data is a header record.

16. The method of claim 7, wherein the combiner data further includes one of a digital signature and a digital certificate.

17. The method of claim 7, wherein the combiner data further includes a digital signature and a digital certificate.

18. The method of claim 7, further comprising

generating a second cryptographic key based at least in part on the at least one label split; and

encrypting the random split with the second cryptographic key, prior to adding the combiner data to the encrypted object;

wherein the random split included the combiner data is the encrypted random split.

19. The method of claim 7, further comprising

before adding the combiner data to the encrypted object, encrypting at least a portion of the combiner data with a header split.

20. The method of claim 19, wherein the header split is constant.

21. A storage medium comprising instructions for causing a data processor to encrypt an object, wherein the instructions include:

generate a cryptographic key by combining a plurality of key splits;

initialize a cryptographic algorithm with the cryptographic key; and

apply the initialized cryptographic algorithm to the object to form an encrypted object;

wherein at least one of the plurality of key splits corresponds at least in part to a biometric measurement.

22. The storage medium of claim 21, wherein the instructions further include:

for at least one of the plurality of key splits, add the at least one key split to the encrypted object.

23. The storage medium of claim 21, wherein the instructions further include:

for at least one of the plurality of key splits, add reference data associated with the at least one key split to the encrypted object.

24. The storage medium of claim 21, wherein the instructions further include:

retrieve at least one of the plurality of key splits from a memory.

25. The storage medium of claim 24, wherein at least a portion of the memory is disposed on a smart card.

26. The storage medium of claim 21, wherein the data processor is distributed, and the instruction to generate a cryptographic key is executed at least in part on a smart card.

27. A storage medium comprising instructions for causing a data processor to encrypt an object, wherein the instructions include:

generate a first cryptographic key by combining an organization split corresponding to an organization, a maintenance split, a random split, and at least one label split;

initialize a cryptographic algorithm with the first cryptographic key;

apply the initialized cryptographic algorithm to the object to form an encrypted object;

add combiner data to the encrypted object, wherein the combiner data includes

reference data corresponding to at least one of the at least one label split and the cryptographic algorithm,

name data associated with the organization,

at least one of the maintenance split and a maintenance level corresponding to the maintenance split, and

the random split; and

store the encrypted object with the combiner data for subsequent access.

28. The storage medium of claim 27, wherein the instructions further include select the at least one label split from at least one credential.

29. The storage medium of claim 28, wherein the selected at least one label split is encrypted, and the instructions further include:

derive a second cryptographic key from a user ID associated with a user, a password associated with the user, and at least one of a unique data instance and a random value; and

decrypt the selected at least one label split with the second cryptographic key.

30. The storage medium of claim 28, wherein the instructions further include:

retrieve at least one credential from a memory.

31. The storage medium of claim 30, wherein the memory is disposed on a smart card.

32. The storage medium of claim 28, wherein the instructions further include generate a time stamp corresponding to a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

33. The storage medium of claim 28, wherein the combiner data further includes a user ID associated with the user.

34. The storage medium of claim 27, wherein the instructions further include generate a time stamp corresponding to at which the object was encrypted, wherein the combiner data further includes the time stamp.

35. The storage medium of claim 27, wherein the combiner data is a header record.

36. The storage medium of claim 27, wherein the combiner data further includes one of a digital signature and a digital certificate.

37. The storage medium of claim 27, wherein the combiner data further includes a digital signature and a digital certificate.

38. The storage medium of claim 27, wherein the instructions further include:

generate a second cryptographic key based at least in part on the at least one label split; and

encrypt, with the second cryptographic key, the random split, prior to executing the instruction to add the combiner data to the encrypted object;

wherein the random split included in the combiner data is the encrypted random split.

39. The storage medium of claim 27, wherein the instructions further include

prior to executing the instruction to add the combiner data to the encrypted object, encrypt at least a portion of the combiner data with a header split;

40. The storage medium of claim 39, wherein the header split is constant.